Age Verification as a Shield for Minors on the Internet
A Quixotic Search?

Francoise Gilbert[1]
IT Law Group - www.itlawgroup.com
Palo Alto, California

On the Internet, no one knows you are a dog.[2] In many instances, the anonymity and openness of the Internet environment allow anyone to easily register as a user on a site using a different name and identity than the actual ones. Generally, one only needs an email address. Free email addresses can be obtained from numerous services, such as Gmail, Hotmail, Yahoo, and others. A savvy 12-year old, after having obtained a free email account, can easily register with a different name and identity, misrepresent her age as being 19 or 22, and obtain the user ID and passwords necessary to register on a social networking site, a virtual world or an online liquor store site. Conversely, it is also easy for an adult to pass himself as a tween or teenager, and obtain the user ID and passwords he needs to use a site aimed at children or minors.

While the existence of child predators, pedophiles and others is not a recent phenomenon, the ease of access to social networking or other sites that offer interaction between members has provided an additional venue for encounters between adults and minors in unsupervised environments. This freedom and anonymity have allowed adults to meet minors online, move the relationship off-line, and initiate sexual activities prohibited by law. On the other hand, there is no doubt that before social networking facilitated encounters, minors or adults interested in pursuing similar types of relationship or illegal activities were able to find willing partners in the brick and mortar world.

Governments and legislators are looking at age verification and similar procedures to protect children from inappropriate material or contacts on the Internet and keep them out of sites aimed at adults. Is it possible to achieve this goal? Are there more reliable and less intrusive alternatives? This article explores some of the issues raised by age verification and looks at the status of laws and government enforcement actions that focus on keeping children and minors out of sites that are not intended for them, or not prepared to handle them.

1. BACKGROUND

a. Doe v. SexSearch.com

The case ***John Doe v. SexSearch.com***[3] provides a typical example of encounters that may result from the use of social networking sites where there is no verification of the age or other information provided by a registrant. SexSearch.com is a website offering an online adult

---

[1] *Françoise Gilbert is a principal of the IT Law Group, www.itlawgroup.com, a law firm based in Palo Alto, CA. Her practice focuses on information privacy and security and data governance. She has assisted global and local companies on a wide range of data protection, data governance, and compliance issues. Ms. Gilbert can be reached at: (1) 650-804-1235 or fgilbert@itlawgroup.com*

[2] *Peter Steiner cartoon published in The New Yorker, page 61 of July 5, 1993 issue (Vol.69 (LXIX) no. 20).*

[3] *John Doe v. SexSearch.com, Case. No. 3:07 CV 604 U.S. Dist. Ct N. District of Ohio.*

dating service which encourages its members to meet and engage in sexual encounters. Members are permitted to provide information for a profile, which consists of a list of responses to specific questions posed by the website. Members may also upload photographs and video content to their profile. John Doe became a member of SexSearch.com, and shortly thereafter located Jane Roe's profile, which provided Jane Roe's birth date, her age (18), and an authentic image of Jane Roe at her then-current age. After chatting online through SexSearch.com, the two decided to schedule a sexual encounter to take place at Jane Roe's home. The meeting went as planned, and the two engaged in consensual sexual relations. However, it turned out that Jane Roe was actually 14 and not 18. A few weeks later, John Doe was arrested and charged with engaging in unlawful sexual conduct with a minor, which exposes him to 15 years in prison, and a classification that might include life time registration as a sex offender.[4] In *John Doe v. SexSearch.com*, the plaintiff sued the social networking site for having failed to adequately screen the minor during the registration.

2. US LEGISLATIVE ACTIVITY

The risks to which children and minors are exposed when using social networking sites, such as Facebook or MySpace, virtual worlds such as Second Life, or other sites such as SexSearch.com, have prompted numerous legislators to introduce bills aimed at increasing the protection of children and minors who use these sites.

a. Federal Legislation

In September 2008, the US President signed into law two bills that address the protection of children online. Senate Bill S. 431 requires all sex offenders to register their email address and other Internet identifiers with the National Sex Offender Registry, and allows social networking sites to compare their records against the database. Senate Bill S. 1738 creates reporting requirements for electronic communications service providers and remote computing service providers who discover content, correspondence and other illegal activities related to child abuse and child pornography.

▪ KIDS Act

Introduced by Senator Charles Schumer, and co-sponsored by Senator Obama and Senator McCain, Senate Bill S. 431, ***Keeping the Internet Devoid of Sexual Predators Act of 2008*** – or "**KIDS Act of 2008"** – requires sex offenders to list with the National Sex Offender Registry all Internet identifiers that they use.[5] The term "Internet Identifier" includes email address and other designations used for self-identification or routing in Internet communications or postings. The new law specifies requirements for keeping this Internet identifier information current. This information is exempt from public disclosure. The law requires the US Attorney General to maintain a secure system to allow social networking websites to use this system in order to conduct searches as frequently as the Attorney General may allow. S. 431 authorizes the US Attorney General to deny, suspend, or terminate use of the system by a social networking website for misuse. The Attorney General and the social networking sites are prohibited from revealing to the public any list of the identified sex offenders.

---

[4] *Information from Memorandum Opinion and Order, Judge Jack Zouhary, document No. 153 filed August 22, 2007.*

[5] *Senate Bill S. 431 will become Public Law 110-400.*

Section 3(5) and 3(6) of the KIDS Act provide limitations of liability for the benefit of the social networking sites. Section 3(5) exempts social networking websites from civil claims arising from the use of the National Sex Offender Registry unless the social networking website engages in actual malice, intentional misconduct or reckless disregard to a substantial risk of causing injury. Section 3(6) clarifies that social networking sites are not required to use this system, and that no federal or state liability, or any other adverse consequence may be imposed on a website based on its decision not to use the information provided in the Registry.

- **PROTECT Our Children Act**

Introduced by Senator Joseph Biden and co-sponsored by Senator Obama, Senate Bill S.1738 "***Providing Resources, Officers and Technology to Eradicate Cyber Threats to Our Children Act of 2008***" or "**PROTECT Our Children Act of 2008**" requires the Department of Justice to develop and implement a National Strategy for Child Exploitation Prevention and Interdiction, to improve the Task Force on Internet Crimes Against Children, and make other improvements to increase the ability of law enforcement agencies in order to investigate and prosecute child predators.[6]

The PROTECT Our Children Act creates reporting requirements for electronic communication service providers and remote computing service providers when they obtain actual knowledge of activities that relate to the sexual exploitation of minors, selling or buying children or child pornography, the use of child pornography, or the use of misleading domain names that lead to pornographic sites.[7] To the extent that the service provider has information about the involved individual, it must provide the identity of the individual who appears to have violated the law, his email address, IP address, URL, and other identifying information.[8]

Failure to abide by this obligation exposes the service provider to a fine of up to $150,000 for an initial violation, and up to $300,000 for subsequent violations.[9] There is, however, no requirement to actively monitor any use by a subscriber or customer, or the content of any communication, or to affirmatively seek facts and circumstances evidencing the use of pornography or child abuse.[10] The law shields from civil or criminal prosecution a service provider or domain name registrar that files these reports or preserves evidence associated with the prohibited activities.[11]

b. State Legislation

The State legislators have been very active, as well. Numerous bills requiring age verification measures on websites were proposed, such as in North Carolina and Connecticut in 2007,

---

[6] *Senate Bill 1738 will become Public Law N. 110-401.*

[7] *PROTECT Our Children Act Section 501(a), which creates a new section 18 US 2258A of the US Criminal Code; to be codified as 12 USC 2258A (a).*

[8] *PROTECT Our Children Act Section 501(a) to be codified as 12 USC 2258A (b).*

[9] *PROTECT Our Children Act Section 501(a), to be codified as 12 USC 2258A (e).*

[10] *PROTECT Our Children Act Section 501(a), to be codified as 18 US 2258A (f).*

[11] *PROTECT Our Children Act Section 501(a), to be codified as 18 US 2258B(a).*

and Georgia[12], Illinois,[13] Iowa[14] and Mississippi[15] in 2008. In addition, bills mandating that convicted sex offenders register their e-mail addresses with the state were also introduced by Kentucky, Virginia, and Arizona legislators.

3. FOREIGN ACTIVITIES

Abroad, several countries have issued recommendation and guidance on the protection of children online in connection with access to social networking.

a. United Kingdom

In April 2008, the United Kingdom government issued the country's first social networking guidance for the industry, parents and children, aimed at helping teens and tweens interact safely on the Internet.[16] The comprehensive report was prepared by a task force of the Home Office on online children protection. It recommends that social networking websites offer strong privacy protection procedures, and use identity authentication measures.

This guidance comes at the time when a study conducted by the country's Office of Telecommunications released a report showing that more than 25% of the country's 8 and 11 year old children have setup a profile on social networking sites even though age restrictions may be in place to prevent pre-teens from accessing such sites.[17]

The recommendations of the Taskforce on Online Child Protection[18] aimed at online social networking sites include:

- Make safety information for users, parents and caretakers, prominent, easily accessible and clear;
- Make safety information available during the registration process prominent on the homepage and in appropriate places within the service, such as in a welcome message;
- Address individual responsibilities to respect and protect the online community, such as how to behave responsibly when posting images and comments;
- Provide information that is specific to the service being provided, updated to reflect service development, and effective and relevant for users;
- Provide instructions for tools that can help users protect their privacy and prevent unwanted contact or communication, such as 'Ignore' functions; removing people from their 'friends' or contact list; and how to review and remove unwanted comments on their site.
- Where possible and appropriate, request and validate personal information from users, e.g., full name, date of birth and/or a valid email address in order to minimize

---

[12] *S. 59.*

[13] *HB 4874.*

[14] *HF 2202.*

[15] *HB 2586; died in Commission.*

[16] *http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance.*

[17] *http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf.*

[18] *http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance.*

the risk of impersonation and enable the service providers to protect younger users.
- Capture an IP address or unique identifier (for mobile devices) with a date and time stamp at registration, regularly refreshed with repeated use of the service, including at each login, with a date and time stamp.
- Screen or review user profile photos, especially for users under the age of 18, using human and/or technical moderation, and remove inappropriate or sexually provocative images or videos posted by users.
- Create reporting mechanisms that automatically capture essential information and relevant evidence, such as a "screen capture" of abusive or inappropriate content, the online ID of the abuser, and the time and date of the incident.

b. Spain

In 2008, the Spanish Data Protection Agency published a privacy handbook for children and parents with recommendations on using appropriate safeguards while online.[19] The handbook provides a basic overview of the fundamental data protection principles set forth in the Spanish Data Protection Act. It addresses the special protection of children's privacy rights. For example, parental consent is required for processing of data for children under the age of 14. The handbook also addresses the privacy risks to which minors are exposed, and provides recommendations. For example:

- Minors should be taught how to use the Internet in a suitable manner to avoid any potential privacy risks.
- Parents should provide guidance to their children regarding the use of Internet, cautioning them on ancillary risks and making sure they do not post or share personal data or personal photos with strangers.
- Parents should raise their children's awareness and caution them on the benefits and drawbacks of the information society.
- Parents should closely supervise their children when using the Internet, ensuring access to adequately protected sites and refusing to provide personal data when there are not sufficient safeguards in place.
- Public forums, chat rooms and social networks are particularly risky environments for minors. Parents should advise their children on the risks of these environments and instruct them to be careful and cautious when online.
- Personal data should always be provided under parental supervision.

The handbook addresses the importance of the protection of children's privacy within the home environment. Children's rights to privacy at home should be kept in mind at all times. Monitoring of their personal computers should be done only when absolutely required and by way of special user accounts with certain restrictions.

4. New Rules Affecting Social Networking Sites

Child predators and others have misused social networking sites in ways that might not have been contemplated by the founders of these sites when they originally designed their sites and outlined the concept. Numerous cases of underage sex encounters were reported. However, families have found it difficult to find ways to protect their children.[20] Meanwhile, in

---

[19] *http://www.ibls.com/internet_law_news_portal_view.aspx?s=sa&id=1426.*

[20] *See, e.g., Doe v. MySpace discussed in the following section.*

addition to bills introduced by State legislators, State Attorneys General have initiated investigations against major social networking sites. In the United States, these investigations culminated with settlements between MySpace and Facebook and a coalition of State Attorneys General. These settlements provide a useful set of guidelines for social networking and other sites (such as virtual world, or multi player game sites) that provide for social interaction amongst users.

a. Unsuccessful Negligence Suits for Shortcomings of Registration Process

Victims of child predators have had trouble finding relief when attempting to hold the social network site responsible for having failed to prevent minors from lying in order to register on their sites. For example, in May 2008, the U.S. Court of Appeals for the 5th Circuit ruled in favor of MySpace in a suit filed by a minor who had been assaulted by an adult whom she had met through MySpace.[21]

The plaintiff, Julie Doe, despite being 13, had registered on MySpace, representing that she was 18 years old. She met a sexual predator online, and was assaulted after arranging a face-to-face encounter. Julie Doe sued MySpace, arguing that the social networking site was negligent for not having implemented technological safeguards that would have prevented her registration and the subsequent meeting.

The Court ruled that the Communications Decency Act immunizes the social networking site from liability on claims that it was negligent in not protecting underage users from online child predators.[22] The court reasoned that an argument that MySpace was liable in negligence for abuse stemming from posted content was essentially an argument that MySpace was liable for the content itself. The court found that immunity under the Communications Decency Act extends to the presence of third-party content and the consequences of that content.

b. MySpace

Concurrently, State Attorneys General were actively pursing the issue with major social networking sites, and conducted investigations in connection with the use of the site networking capabilities by child predators, sex offenders, and others in order to meet with underage individuals for sex or to sell pornographic material. In January 2008, MySpace settled with 49 State Attorneys General after such investigations.[23]

In the settlement, MySpace agreed to implement design and functionality changes to its site, and to develop education and tools for parents, educators, and children. MySpace will cooperate with law enforcement to deter and prosecute criminals misusing the Internet, and develop a new set of privacy protection standards.

---

[21] *Doe v. MySpace Inc., 5th Cir., Case No. 07-50345, May 2008, affirming a 2007 decision of the U.S. District Court for the Western District of Texas. See also BNA Privacy & Security Law Report, June 2, 2008.*

[22] *Section 230 of the Communications Decency Act provides: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1).*

[23] *See attachment to North Carolina Attorney General Press Release at http://www.ncdoj.com/DocumentStreamerClient?directory=PressReleases/&file=AG%20Cooper%20MySpace%20agreement.pdf.*

A major component of the settlement is the commitment to hire a third party to compile a registry of email addresses provided by parents who want to restrict their children's access to the website. MySpace will bar anyone using an email address listed in the registry from signing up or creating a user page profile. In addition, MySpace agreed to work to improve the algorithm used to check for underage users.

In order to protect members under 18, MySpace will automatically change the default setting from "public" to "private" for profiles of users under 18, and restrict requests from others to be their "friends". It will keep closed a section of its site called "high school" for users under 18, so that users under 18 can block all users over 18 from viewing their profile or contacting them. Users over 18 will only be able to search the high school section for students who are graduating in the current or upcoming year. Further, users over 18 will not be able to add users under 16 as friends unless they know the younger user's last name or email address.

MySpace.com will include new privacy protections for all users, allowing them to establish a "private" setting for their profile, and block others from contacting them. MySpace also committed to devote more resources to online privacy and safety efforts and to better respond to user complaints. It will implement a 24-hour hotline to respond to inquiries from law enforcement officials. Sex offenders will be removed from the site. A third party will identify and expunge inappropriate images, and regularly sever any links between the site and the pornographic websites.

In addition to the above measures, MySpace will organize, with the support of the Attorneys General, an industry-wide Internet Safety Technical Task Force devoted to finding and developing online safety tools and online authentication tools and to establish specific objective criteria that will be used to evaluate technology safety solutions. AOL, ATT, CDT, Facebook, Google, Linden Lab, Microsoft, MySpace, Verizon, and Yahoo! have joined this taskforce.

c. Facebook

Facebook has had dealings with the State Attorneys General similar to those of MySpace. In October 2007, Facebook settled an investigation with the New York Attorney General, in which it agreed to provide notice of its safety procedures on its website. Facebook will establish an independent address to receive complaints about inappropriate content (pornography) and conduct. It committed to address these complaints within 24 hours, and to provide a report to the person who submitted the complaint about the steps taken within three days of receipt of the complaint.

In addition, in May 2008, Facebook entered into a settlement with 49 State Attorneys General, which is similar to the MySpace settlement. In this settlement, Facebook agreed to add more than 40 safeguards to protect young users from sexual predators and cyber bullies. It will ban convicted sex offenders from the site and will limit older users' ability to search online for subscribers under 18.

Like MySpace, Facebook has agreed to build a taskforce seeking ways to better verify users' age and identity. Facebook will ensure that companies offering services on the site comply with the new safety and privacy guidelines. In particular, Facebook will keep tobacco and alcohol advertisements from users too young to purchase the products and will remove groups whose comments or images suggest that they involve incest, pedophilia, or other inappropriate content. Moreover, the company will send warning messages when a child is in

danger of giving personal information to an adult. Facebook will also review user's profiles when they ask to change their age, ensuring that the update is legitimate, and not intended to let adults masquerade as children.[24]

5. OTHER EXISTING LEGAL MODELS

In the United States, laws, regulations, and best practices have been in place for several years to attempt to protect children from the dangers of venturing into the adults' world. One of the most important laws in this area is the **Children Online Privacy Protection Act ("COPPA")**.[25] COPPA is limited to the protection of minors under 13.

a. Children Online Privacy Protection Act

COPPA applies to websites that are directed to children under 13 or have actual knowledge that children under 13 use the site. The law regulates the collection online of information about a child, such as full name, home address, email address, and hobbies. The protected information also includes information collected through cookies and other types of tracking mechanisms when they are tied to individually identifiable information.

The law requires websites to identify users who are under 13. When a user is identified as under 13, the interaction with the children and the collection, use, or retention of the child's data must be conducted in a manner consistent with the requirements of the law and its related Children Online Privacy Protection Rule.

In order to determine a user's age several mechanisms are considered "best practice". In general, websites must use an age screening mechanism that asks users to provide age in a way that does not invite falsification (neutral age-screening). For example, a drop down menu for users to enter the year of birth would be good. However, a drop down menu that allows users to enter birth years only making them 13 or older would not be considered neutral. A check box stating, "I am 12 years old" would not be considered neutral, as well. On the other hand, a temporary or permanent cookie might be used to prevent users from back buttoning and entering a new age to circumvent the screening mechanisms.[26] The law and its regulations do not suggest specific mechanisms or technologies.

- **Verifiable consent under COPPA**

COPPA also requires that, before collecting, using, or disclosing personal information from a child, an operator must obtain verifiable parental consent from the child's parent. The operator must make reasonable efforts, taking into consideration available technology, to ensure that, before personal information is collected from a child, a parent of the child receives notice of the operator's information practices and consents to those practices.

The Federal Trade Commission ("FTC") uses a "sliding scale" approach to parental consent.[27] The required method of consent varies based on how the operator uses the child's

---

[24] *See Facebook efforts at educating its users: http://www.facebook.com/help.php?page=419.*

[25] *15 U.S.C. § 6501-6506 (Pub. L. 105-277, enacted October 21, 1998).*

[26] *Children's Online Privacy Protection Rule, http://www.ftc.gov/os/1999/10/64fr59888.htm; FTC Kidz Privacy, http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html.*

[27] *16 CFR Part 312, Children's Online Privacy Protection Rule; final rule amendment, http://www.ftc.gov/os/2005/04/050420coppafinalrule.pdf.*

personal information. If the operator discloses the information to others, a rigorous method of consent is required. If the operator uses information for internal purposes, a more liberal method of consent is required.

If the operator wants to disclose a child's personal information to third parties, the methods of consent required include:

- Written consent: Obtaining a signed form from the parent via postal mail or fax
- Phone call: Taking calls from parents through a toll-free telephone number staffed by trained personnel
- Credit card: Accepting and verifying a credit card number in connection with a transaction
- Email accompanied by digital signature

Unfortunately, this provision fails to recognize that payment cards can be issued to minors and that merchants have little ability to verify that the card was issued to a minor or do not want to pay the fee that a service would charge to provide this information.[28]

▪ Other COPPA Requirements

In addition to the above, COPPA requires two types of notices. One notice is to be addressed to the children, and the other type of notice is to be addressed to their parents or guardian. The notice of information practices that is addressed to children must be readable by children. It must be clear and easy to understand. It must provide information regarding the information that is collected on the site and the required participation of the child's parent or guardian.

The notice of information practices that would be intended for the parents must explain to the parents that they have the right to access to, and control over their children's information. Of course, concurrently the company must provide the parents with this access and control.

b. Enforcement of COPPA by the Federal Trade Commission

The Federal Trade Commission has aggressively prosecuted websites used primarily by children when these sites had aggressive data collection practices. The FTC has several avenues for prosecuting companies for their data collection, use, and sharing practices that affect the privacy of young children. The FTC may bring enforcement actions and impose civil penalties for violation of COPPA. In addition, the FTC retains its authority under Section 5 of the FTC Act to examine practices for deception and unfairness.

A practice would be deemed "deceptive" under Section 5 of the FTC Act if it is likely to mislead and affects behaviors or decisions about a product or service. It would be deemed "unfair" if it causes or is likely to cause substantial injury, not outweighed by other benefits, and not reasonably avoidable.

Since the late 1990's, the FTC has conducted numerous enforcement actions against sites whose practices with respect to children information were questionable. Its enforcement action against Xanga has been one of the most spectacular because of the amount of the fine assessed against the company.

---

[28] *Personal conversation with a provider of payment cards to minors. October 2008.*

- **US v. Xanga.com Inc. (2006)**

The Xanga enforcement action, in 2006, resulted in the largest fine ever assessed by the FTC against a site in connection with the protection of children's information: $1million. In this case, although the Xanga site sign-up process stated that children under 13 could not join, the Site allowed visitors to create Xanga profiles even if they provided a birth date indicating that they were under 13.

The consent degree between the FTC and Xanga required Xanga to delete all information obtained in violation of COPPA. The company must also distribute COPPA compliance literature to personnel and post links to educational materials on its site for 5 years.

The Xanga consent decree specifies numerous reporting requirements, which indicate the type of documents and activities that the FTC considers important in the management of a website when a substantial portion of its users are children. Xanga will have to keep the FTC apprised of the criteria and process used when the site registers visitors online for any activity requiring the submission of personal information. It will also have to provide the FTC with copies of the site privacy notices and privacy notices sent to parents. In addition, Xanga will provide to the FTC on a regular basis descriptions of the methods used to obtain parents verifiable consent and the methods provided for parents to review personal information collected from children. Moreover, Xanga must clarify why each type of information collected from children is necessary for the provisions of the particular activity, and identify the procedures used to protect the confidentiality, security, and integrity of the information.

- **FTC v. Industrious Kids and www.imbee.com (2008)**

In March 2008, the FTC completed an enforcement action against www.imbee.com, a social networking site operated by Industrious Kids especially targeting children ages 8 to 14. In its complaint, the FTC stated that www.imbee.com collected personally identifiable information before providing notice to parents, or obtaining their consent. The company only sent a request to the parent after having collected the child's information, and kept information even if no consent was given.

The consent decree requires the site to pay $130,000 in civil penalties and to destroy all information collected in violation of the rule. In addition, it must include conspicuous notices and links, throughout its site, to invite users to visit the FTC materials about protecting children's privacy online (http://www. ftc.gov/privacy) and the social networking tips for parents and youth site (http://onguardonline.gov/socialnetworking). Industrious Kids will also have to provide the FTC with reports on the operation of its site for three years.

c. State action under COPPA

The Texas State Attorney General, who is the only State Attorney General who elected not to participate in the nationwide consent decrees with MySpace and Facebook, has taken personal initiatives in connection with the protection of children online. In April 2008, the Texas State Attorney General completed an action under COPPA, in the case *Texas v. Doll Palace Corp.* W.D. Tex. (Texas April 2008). In this case, the site required users, as part of the sign-up registration process, to provide their age. The users were then presented with a screen stating "The site requires that you have permission from a parent if you are under 13. Do you have a parent with you now?" Following the statement, the user was required to click a "yes" or "no" box in order to continue. The Texas Attorney General found this practice questionable, and stated that:

"*Companies cannot take on a veil of innocence by hinting to underage users ways to bypass age verification requirements*."

d. Children's Internet Protection Act

The **Children's Internet Protection Act** or "**CIPA**"[29] requires schools and libraries using the E-Rate Discount[30] to use technology protection measures with respect to any of their computers with Internet access, in order to prevent access to visual depictions that are obscene, child pornography or harmful to minors. This technology protection measure must be used when the computers are used by minors. The library may disable the protection during use by an adult, to enable *bona fide* research and other lawful purposes.[31]

e. Child Registry Laws

In addition to the Federal laws aimed at protecting children, States have taken numerous initiatives, as well. Utah and Michigan have addressed the protection of minors from solicitations for the purchase of illegal products or substances (such as alcohol) by enacting their Child Registry Laws in 2005.

Both of these laws allow individuals to register "contact points" of minors (<18). These contact points include email address, phone number, and fax number. The laws prohibit sending a communication to a contact point that is registered in the State Registry if the communication advertises a product or service that a minor is prohibited by law from purchasing, or that is harmful to minors (as defined in the State law): gambling, pornography, alcohol, tobacco, and illegal and prescription drugs.[32] Violations of these laws are subject to stiff penalties including prison and fines. The prohibition applies even if the communication is otherwise solicited.

The Registries that maintain the lists of "contact points" are kept under the authority of the State of Utah and State of Michigan. Marketers who wish to advertise products or services that are covered by the law must compare their list against the registry list before sending their emails.

6. ELECTRONIC AUTHENTICATION

To date, the legislators have stayed away from age verification, and have opted to address the issue of child predators and dangers of social networking through measures that would prevent sex offenders from accessing the sites. There are many other powerful ways available, such as electronic authentication. Age verification mechanisms are currently

---

[29] *Pub. L. No. 106-554*

[30] *The E-Rate discount is a discount granted to libraries and schools when they purchase Internet access and computers.*

[31] *The constitutionality of the Children's Internet Protection Act was challenged on First Amendment grounds in the case American Library Association v. United States filed in Pennsylvania. After appeals, the case was reviewed by the U.S. Supreme Court in 2003. The Court held that the use of filtering software by libraries does not violate their patrons' First Amendment right, and that CIPA does not induce libraries to violate the Constitution.*

[32] *Interestingly, the legal drinking age in the United States is 21. The Child Registry Laws would not shield individuals between 18 and 21 from offers to purchase alcohol even though it is illegal for them to purchase alcohol.*

available in commerce. They have been marketed, for example, to websites that sell alcohol online, so that a site has a means to verify that the purchaser of alcohol is meeting the drinking age requirements.[33]

The use of these technical means for age verification poses serious technical and legal problems.[34] In order to be able to verify the age of a person an organization is likely to need access to additional information about the identity of the person. Then, once a person's identity is determined, it is necessary to use the proper tools to authenticate the person when the individual returns to the site. These two phases are known as "identification" and "authentication process".[35]

During the *Identification* phase, an organization will need to determine who a specific person is. This is done with associating attributes – such as name, address, social security number, gender, date of birth – with a person. Once the identification process has determined enough about a person that the company is willing to do business with him – such as granting him access to its site – an *authentication* process is used when someone purporting to be that person seeks remote access. Authentication involves verifying that the person trying to access the system is really the person who was previously identified.[36] In most cases, the identification process will require the participation of one or more third parties (identity providers) who can provide the required identity information. In the case of a social networking site, it could be a school, a parent, or a third party.

Identity verification through electronic authentication poses numerous legal questions that are beyond the scope of this article. For example, the identification process requires the collection of personal information by the identity provider, and the disclosure of this information to the social networking site (relying party). What information is collected by the identity provider? How much of this information may it disclose to the relying party?

The nature of the assertion made about a person will also have to be defined precisely. Does the assertion cover just the age of the person, or does it cover as well the person's name, address or professional or other qualification? What security measures should be used for the protection of the information? The collection process and the use of the collected information will be subject to the applicable information privacy and information security laws. There may be data retention requirements or prohibitions. If information is transferred across borders, foreign laws restricting the transfer of information outside a country may apply.

There are also liability concerns. What happens if there is a faulty authentication and the applicant is granted access to the site or to the system when he should have been excluded? Who will bear the risk associated with a faulty authentication?

The concepts of federated identity management, user authentication, and age verification are still in their infancy. They will require further legal analysis and scrutiny.

---

[33] see, e.g. IDology Inc, at, http://www.idology.com/. See also, ChoicePoint, http://www.choicepoint.com/products/age_verification.html.

[34] See, e.g., OECD Recommendation on Electronic Authentication, and OECD Guidance for Electronic Authentication, http://www.oecd.org/dataoecd/32/45/38921342.pdf.

[35] Thomas J. Smedinghoff and David A. Wheeler, Addressing the Legal Challenge of Federate Identity Management, BNA Privacy & Security Law Report (March 3, 2008)

[36] Id.

7. OTHER COMPLEX ISSUES

There are many issues surrounding the concept of age verification.[37] Verifying a person's age is likely to require access to more information than just age so that the person is authenticated. When the disclosure of a person's identity is required, numerous privacy and security concerns arise. There are also concerns about errors, the consequences for these errors (data spills, people being wrongfully accused, identity theft) and the liability for these errors. There are, as well, broader questions about human rights and society in general.

a. Data security and data control

New laws are requiring website owners to scrub their databases against public databases in order to identify which of their users must be removed or denied entry. In order to be able to verify that an individual is not part of an excluded category, databases will have to be created. Who would be responsible for managing these databases? Which security measures would have to be used to protect this information? Would information be stored on large databases belonging to private companies contracted for such work? What access, if any, would consumers have to this information? How efficient would these databases be since most people have several email addresses? How would errors be identified and corrected?

b. How to ensure adequate authentication and identification

In order to be effective and efficient, age verification systems require the collection of some type of personal information. As such, it is privacy invasive. In order to protect children, should adults only be "tagged", so that an individual would be deemed a child if he / she is not listed on the databases? What would be the content of such a database, and how much information would be required to authenticate a person and label that person an "adult"?

Moreover, when applied to children, information such as social security numbers might not be available to authenticate age. Children do not necessarily have a social security number. Nor do they have credit reports or bank accounts against which to verify information. If none of this information is available, or if there is a concern that collecting this information would open the door to more identity theft or other risks, how could children be identified? Would the involvement of their parents be required? Would the schools be also an appropriate vehicle to provide identity? Is this feasible and is this desirable?

c. Duration of the authorization

Age verification may work at the time of the initial registration, but how about the other uses of the site? Once a user has been authenticated and provided a user name and password, how do we know with some certainty that the individual who logs in on a site with a certain username and password is the same as the one who initially signed on and provided personal details? Can a site with reasonable access control procedures know that the person who logs on under Juliana's user name is still Juliana after the site has validated once that there is in fact a 25-year-old named Juliana? Individuals, especially children, are notorious for sharing passwords and user ID. In many households, the entire family shares one computer. Different users might not have different accounts. Could Juliana's little brother who

---

[37] *See, e.g., MySpace Coming of Age for Coming of Age, Leslie Harris, Center for Democracy and Technology; http://abcnews.go.com/Technology/story?id=4355851&page=1. See also: http://www.cdt.org/press/20080228press.php.*

uses the family computer after his older sister Juliana benefit from the settings of the older sister's account?

d. Privacy and Anonymity

Even if all websites were classified or labeled "PG 13" or "R" like movies or video games are, and if it were possible to create a technical solution that would be easy to implement, there would remain the problem of balancing the legitimate individual rights and freedoms against the need to protect children from predators or from content that might not be suited to them. Identification requires knowledge of, and access to personal data. Would it be possible to have robust age verification, but still protect privacy? Would Internet users, regardless of age, be required to register and login wherever they go? Would an adult who wants to check Club Penguin before registering his children to the service have to provide detailed identification so that Club Penguin verifies that this father is not otherwise a child predator or a pedophile? If this were the case, where would the boundaries be set? Would the right to access information anonymously be undermined?

e. Constitutional law or Human Rights issues

The Constitutions of many countries provide the citizens and residents of these countries with extensive rights. Would excluding minors from social networking sites, virtual worlds, multiplayer gaming sites, and the like violate the children's constitutional rights to free speech (in the US) or similar rights? Would age verification aimed at minors, but necessarily required of all users, pass constitutional scrutiny if it burdens the free expression of adults?

In the United States, the Communication Decency Act of 1996,[38] which attempted to regulate pornographic material (when available to children) on the Internet has been partially overturned. The indecency provisions were held to be an unconstitutional abridgement of the First Amendment Right to Free Speech because they did not permit parents to decide for themselves what material was acceptable for their children.

Similarly, the "Children Online Protection Act" or "COPA" (not to be confused with the Children Online Privacy Protection Act or COPPA)[39] was adopted to restrict access by minors to any material defined as harmful to minors on the Internet. COPA has been repeatedly struck down by courts on the grounds that the law violates the constitutional right to free speech under the First Amendment to the Constitution of the United States.[40]

f. What limits to the proposed silo system?

Most age verification schemes currently contemplated might end-up establishing silos to separate children from adults, in order to prevent adults from entering a world dedicated to children, and children from accessing adult only content. Is this a good thing? How does this compare with daily life where children, teens, young adults, adults and seniors constantly interact with each other?

---

[38] *47 U.S. § 223.*

[39] *47 U.S.C. § 231.*

[40] *See also the (unsuccessful) challenges to the Children's Internet Protection Act, above, on grounds of First Amendment violation.*

8. GLOBAL ISSUES

There are more issues, which stem from the global reach of the Internet. If age verification technologies were efficient, cost effective, and available, would they achieve the goal of protecting children from adult content, and would these shield children from predators? Given that the Internet can be accessed from anywhere in the world, would barriers created in one country prove to be useless or inefficient in a global economy? There are indeed major hurdles.

a. Worldwide cooperation needed

First, age verification legal regimes are likely to be poorly adapted to the global reach of the Internet. Social networking sites, virtual worlds, and similar sites are accessible from almost anywhere in the world. A country-centric age verification regime would fail when minors can access foreign-based websites located in more permissive legal regimes. Children and minors from countries that hamper their access to prohibited sites are likely to flock to foreign sites with less restrictions. Unless all countries cooperate in creating a global age verification regime, teens and others trying to avoid age verification will seek access to foreign sites that are subject to less restrictive laws.

b. Which definition of "Majority"?

Furthermore, even if each country agreed to create an age verification regime to bar minors from accessing certain sites – or certain areas of a site –, the countries would have to agree on thorny definitions. How would "minor" be defined? In general, "majority" is defined as the age of consent and legal responsibility. There is no consensus globally about the age of majority. Most countries have adopted 18 as the age of majority. However, in Japan, Taiwan, Thailand, and the Republic of Korea, the age of majority is 20. In Singapore, Monaco, Honduras, or Egypt, it is 21. The same disparities appear in the United States. While the age of majority is 18 in most US states, it is 19 in Alabama and Nebraska, and 21 in the District of Columbia and Mississippi.[41]

There are additional complexities when looking at specific areas where minors and adults are subject to different regimes. The age of consent is only one facet of the concept of majority. Consider, for example, the drinking age. In most countries, the legal drinking age is 18, but it is 21 in the United States, and 16 in France, Germany, Italy, Belgium, and Portugal.[42]

The definitions of what constitutes "sexual assault" or "statutory rape" vary extensively as well. In the United States, the age of consensual sex varies from 14[43] to 18.[44] For example, in Texas, while the age of majority is 18, a sexual encounter with a 14 year old might not be illegal. Section 22.011(e) of the Texas Penal Code provides an affirmative defense to a charge of sexual assault if the victim is over 14 and the actor is less than three years older than the victim.[45]

---

[41] *Wikipedia: http://en.wikipedia.org/wiki/Age_of_majority.*

[42] *Wikipedia: http://en.wikipedia.org/wiki/Legal_drinking_age.*

[43] *South Carolina. http://www.livestrong.com/article/12483-age-consensual-sex/*

[44] *http://www.livestrong.com/article/12483-age-consensual-sex/.*

[45] *Section 22.011(e) provides:*

> *(e) It is an affirmative defense to prosecution under Subsection (a)(2) that:*

With such disparities between countries, and such varieties of matters subject to age requirements, the implementation of a global age verification regime becomes highly problematic. How could a website enforce an age verification regime when there is no consensus about the age of individuals to be protected? In addition, even if a consensus were reached, which law would apply to a particular situation that involves an actor in one country, and a victim in another country?

c. Which content would be restricted?

In addition, in order to implement an efficient age verification regime, it would be necessary to identify the sites, venues, or content to which the restrictions apply. It is likely that there would be discrepancies between the different laws. For example, what type of content would be permitted? Even the mere attempt at defining what is prohibited might prove difficult. The famous words of Justice Potter Stewart "I know it when I see it"[46] as his best attempt at defining what constitutes obscenity are still relevant. Which types of sites would have to create silos? Would the silos apply to all types of information?

A global solution would be even more complex, because countries have different definitions and approaches to issues that are at the center of the problem. What one country may wish to prohibit might be legal in another country. For example, hate speech is a crime in Brazil, but is protected under the First Amendment in the United States. Saudi Arabia bans homosexuality, but it is accepted or legalized in many other countries.

9. Effect on Product Design

The evolution of social networking sites and virtual worlds into places where users of all ages might interact and the related legal, privacy and security concerns, have a direct effect on the design of websites. Site designers must take into account the measures outlined in the MySpace and Facebook settlements when designing, building, or modifying sites directed to a U.S. audience. Indeed, these settlements do reflect the opinions of the State Attorneys General of the United States on the best practices for handling the provision or exchange of personal information, and the interactions between members of social networking sites.

The design of an application for a social networking, a virtual world, or a game site would have to provide the site with the ability to interact with registries where information might be encrypted. It will have to enable the site to evaluate the user's age in order to comply with the

---

(1) The actor was not more than three years older than the victim and at the time of the offense:

(A) Was not required under Chapter 62, Code of Criminal Procedure, to register for life as a sex offender; or

(B) Was not a person who under Chapter 62, Code of Criminal Procedure, had a reportable conviction or adjudication for an offense under this section; and

(2) The victim:

(A) Was a child of 14 years of age or older; and

(B) Was not a person whom the actor was prohibited from marrying or purporting to marry or with whom the actor was prohibited from living under the appearance of being married under Section 25.01.

[46] *Jacobellis v. Ohio, 378 US 184, 197 (1964); Justice Stewart's concurring opinion.*

applicable laws, and the industry guidelines and best practices. For example, if access to registries is not possible, consider multiple questions at the registration stage in order to determine consistency between responses. There might be questions about the users (e.g., school, degrees) that might help infer the age bracket in which the user is situated. If termed appropriately, these questions might not be invasive of the user's privacy.

The site might also wish to use credit card ownership as a method to verify both the identity of the proposed user. The site may consider making the use of a credit card mandatory, in order to evaluate the user's access to credit, as an indicia that the person might be or not a minor. However, having access to a credit card may not be a solid proof of a person's age. Many minors use payment cards or credit cards. The payment cards have been legally issued by their parents who have agreed with a credit card issuer that they would be responsible for the expense that their child charges to the card. Payment cards are only a means of payment. They are not an identification document, and they do not constitute proof that their holder is not a minor.

The site may also need to be equipped with the ability to track users to avoid repeated requests from individuals who are guessing what might be the key to entry. Cookies and digital fingerprinting of the hardware might be useful. The site should also be equipped with technologies that would help monitor unlawful content and suspicious interactions.

10. CONCLUSION

There are numerous societal and other issues beyond the legal issues described above. Is age verification the cure to the problem of child predators? Will it help shield children from access to controlled substances or questionable materials? Can we hope to succeed in identifying and authenticating individuals on the Internet when children's creativity and ingenuity – and adults' complacency – have made it impossible to achieve reliable identification or authentication in the brick and mortar world?

Most countries have laws that set a minimum age for the purchase of liquor or tobacco, or access to restricted material that contains sex, nudity, or violence. Nevertheless, minors find ways to obtain alcohol or cigarettes or view X-rated movies. They ask help from older friends. They procure fake identification documents.

In the brick and mortar world, where it is arguably easier to compare a live person to the photo attached to the persons' identification document, society is struggling to prevent teens from using fake ID documents and other fraudulent means to purchase alcohol and tobacco, or access restricted content. When children use fake identification documents, the clerk at the liquor store does not verify the identity of the person; he only verifies the documents the person provides. How can we expect to succeed in cyberspace where there is even less ability to conduct a reliable identity check?

Social networking sites are a logical – albeit sometimes unfortunate – meeting place for youth and adults. As a matter of public policy, each country will want to establish a system that duplicates the system in place in the brick and mortar world, in order to verify people's age – and possibly identify – before giving them access to restricted areas. Does it make sense to replicate a model that has shown so many flaws?

Age verification might not be the perfect type of protection. It is clear that age verification will not have a 100% success rate. In addition, even if technology might enable a site to identify a user, authenticate him, and ascertain his age, there will always be problems. Further, online verification does not verify the person; it only verifies the documents or proof of identity the person provides. Other problems are bound to emerge as well.

Parents and schools remain the most logical place to turn to. They have an important role to play. Educating children about the dangers that they might encounter on the Internet, and teaching children the appropriate ways to use the Internet would definitely contribute to the better safety of these sites.

// Palo Alto, CA October 2008